



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/734,935

12/12/2003

Michel S. Simpson

26530.92

2224

27683 7590 10/27/2009

HAYNES AND BOONE, LLP

IP Section

2323 Victory Avenue

Suite 700

Dallas, TX 75219

EXAMINER

LEMMA, SAMSON B

ART UNIT

PAPER NUMBER

2432

MAIL DATE

DELIVERY MODE

10/27/2009

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/734,935	Applicant(s) SIMPSON ET AL.	
	Examiner Samson B. Lemma	Art Unit 2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on Pre-appeal request filed on 01/21/2009.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1 and 4-21 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1 and 4-21 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Response to Arguments

1. In view of the Pre-Appeal Brief filed on January 21, 2009, PROSECUTION IS HEREBY REOPENED. New grounds of rejection (for claims 1 and 4-10) are set forth below.
2. The issues regarding anticipation require that terminology used in the claim be clarified so as to have a clear understanding of the issues for appeal.

Appellant's submitted two arguments.

The second argument presented by the appellants was in relation to the limitation recited as "digital signature".

Appellant's on page 3 of the pre-appeal brief argued that what is cited by the examiner is not equivalent to the limitation recited as, "digital signature." However the above argument/s has been fully considered but found to be not persuasive.

In other words what is cited by the Examiner referring to the Carter's reference, the reference on the record, such as, *figure 5, ref. Num "102", "encrypted message digest", signed by the private key. In particular see what is disclosed on column 14, lines 15-21, "the encrypted message digest 102 is formed by generating a message digest based on the current contents of the data portion 94 of the document 90 and then encrypting that message digest with the*

Art Unit: 2432

private key 80 of the member who is signing the document 90.” See also the abstract and column 6, lines 11-12, “collaborative signatures, such that members of the group can digitally sign a particular version of the data portion. These collaborative signatures can then be used to advantage in ways similar to conventional individual digital signatures. For instance, the collaborative signatures can be used to identify the signing member” is found to meet the limitation recited as “digital signature.”

However the first argument presented by the applicant’s regarding the limitation recited as “access control list” in independent claim 1 is found to be persuasive.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. **Claims 1, 4-10** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Stephen R. Carter** (hereinafter referred as **Carter**)(U.S. Patent No. 5,787,175) (Date of patent 28, 1998), in view of **Rider** (hereinafter referred to as **Rider**) (U.S. Patent Publication 2006/0173999 A1) (filed on 08/07/2003, claims priority of a provisional application filed on 08/07/2002) further in view Frey et

Art Unit: 2432

al (hereinafter referred as **Frey**) (U.S. Patent No. 7,017,183 B1, filed on Jun 29, 2001)

5. **As per independent claim 1 Carter discloses a method for controlling access to a document, [Abstract] comprising:**

- **Determining an access right for a user; (Column 12, lines 56-63; column 15, lines 62-67; abstract and column 8, lines 27-29)** (*Access Control Methods FIGS. 4-9 illustrate one method according to the present invention for controlling collaborative access to the work group document 90. In particular, the method includes computer-implemented steps for collaboratively encrypting the document 90 (FIG. 6) and steps for restricting access to the data portion 94 of the collaboratively encrypted document (FIG. 9).*)
- **building a member definition** [*Figure 5, see "member definition"*] **comprising a member identifier** [*Figure 5, ref. Num "98", See "member identifier"*], **an access control** [*See column 12, lines 56-57; column 13, lines 52-62, see figure 5, ref. Num 100, "encrypted document key" signed by the public key of the member. Only the member with the corresponding private key can access the document. In particular see the following which is disclosed on column 13, lines 64-column 14, lines 5, "The encrypted document key 100 is formed by encrypting the document key obtained during the step 110 with the public key of the member in question, which was obtained during the step 116. Note that the underlying document key is the same for each member of the collaborative group, but the encrypted form 100 of the document key is unique to each member. Those*]

Art Unit: 2432

of skill in the art will appreciate. that the encrypted document key 100 can be decrypted only by using the private key 80 that corresponds to the public key 78 used to encrypt the document-key. "See also "collaborative access controller 44" which is described on column 6, lines 11-22 as the access controller which restrict access to the members only. Non members are restricted from accessing the information. See for instance the following disclosed on column 6, lines 11-12, "users who are currently members of a collaborative group can readily access the information, while users who are not currently members of the group cannot"]

and a digital signature,*[See also figure 5, ref. Num "102", "encrypted message digest", signed by the private key. In particular see what is disclosed on column 14, lines 15-21, "the encrypted message digest 102 is formed by generating a message digest based on the current contents of the data portion 94 of the document 90 and then encrypting that message digest with the private key 80 of the member who is signing the document 90." See also the abstract and column 6, lines 11-12, "collaborative signatures, such that members of the group can digitally sign a particular version of the data portion. These collaborative signatures can then be used to advantage in ways similar to conventional individual digital signatures. For instance, the collaborative signatures can be used to identify the signing member."]*

and associating the member definition with the user. *[Figure 5 and column 6, lines 11-22, See "Users who are currently members of a collaborative group can readily access the information, while users who are not currently members of the group cannot"]*

and

Art Unit: 2432

- **Linking the member definition to a portion of a document.** *[Figure 6, ref. Num "120"] ("Link member definition(s) with document.")*

Carter does not explicitly disclose

linking the member definition to a first data portion of a document, wherein the document has the first data portion and a second data portion, receiving a request from the user to access the document; comparing the request with the access right; and allowing access to only the first data portion in accordance with the access right

However, in the same field of endeavor, **Rider** discloses,

Linking the member definition to a first data portion of a document, wherein the document has the first data portion and a second data portion, [paragraph 0044, figure 4A & 0034-0035] *(As shown, document 400 includes descriptor portion 402 and data portion 404. Descriptor portion 402 can include basic information about the device and its operation whereas data portion 404 can include actual data, which can be employed by specific applications. Portion 406 is a portion of data 404 that has its access governed in accordance with the principles of tier two security as described herein. That is, **one or more access rights can be associated with portion 406**. Although one portion 406 is shown, an ordinarily skilled artisan will appreciate that the same or other access rights can govern other portions of data portion 404.)*

Receiving a request from the user to access the document; comparing the request with the access right; and allowing access to only the first data portion in accordance with the access right [Paragraph 0034-0035]

Art Unit: 2432

paragraph 0044, figure 4A] *(On paragraph 0034, the following has been disclose. Moreover, security manager 170 can permit, restrict or completely deny a user **request to access one or more documents** as well as the contents of those documents. A document or a portion thereof can represent a command for, or a configuration of, one of devices 135 such as a router or switch. Security manager 170 governs by determining whether a particular user has access rights to a specific network resource, **a particular document or only a portion of a document. Furthermore on paragraph 0035, the following has been disclosed. “By restricting access in relation to a document's content, a more fine-grained approach to configuring, managing and monitoring network resources is realized. Hence, tier two security restricts a user to data **constituting a portion of an entire document rather than providing complete or no access to that document.** For example, FIG. 4A depicts **document portion 406 that is accessible. Note that other portions of document 400 are not necessarily accessible to that user.**”)***

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the feature such as linking the member definition to a first data portion of a document, wherein the document has the first data portion and a second data portion and receiving a request from the user to access the document; comparing the request with the access right; and allowing access to only the first data portion in accordance with the access right as per teachings of **Rider** into the method as taught by **Carter**, in order to provide a more fine-grained access control to the resources (portions of documents) [See For instance *Rider* on paragraph 0035]

Art Unit: 2432

The combination of Carter and Rider does not explicitly disclose that the access control is actually the "access control list"

However, in the same field of endeavor **Frey at least on column 10, lines 5-11, figure 4, ref. Num "438", column 4, lines 35-40 and figure 1, ref. Num "144" discloses the following** which meets the limitation recited as "access control list". "In accordance with a preferred embodiment, portal database 424 further comprises a user profile table 430, a group profile table 432, a group membership table 434, an object security table 436, and an **ACL (access control list)** sync map 438 (hereinafter synchronization map 438), these tables and maps comprising information as will be described further infra."

Furthermore on column 4, lines 35-40 and figure 1, ref. Num "144", the following has also been disclosed which meets the limitation recited as "access control list" "For each document in that set, the **access control list 144 is checked** to see if that portal user **has access permission to that document**, or if that user is a member of a portal group having access permission to that document. The portal user is only presented with a listing of documents for which they have access permission."

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to employ features such as access control as per teachings of **Frey** into the method of "access control" as taught by the combination of **Carter and Rider**, in order to enhance the security by providing further fine-grained access control to the resources) [*See For instance Frey column 4, lines 35-40*]

6. **As per dependent claim 4 the combination of Carter, Rider and Frey**
discloses a method as applied to claims above. Furthermore, Carter
discloses the method, further comprising adding a new user to the
document. *[Figure 7, column 7, lines 3-5] (“adding a new member”)*
7. **As per dependent claim 5 the combination of Carter, Rider and Frey**
discloses a method as applied to claims above. Furthermore, Carter
discloses the method, further comprising removing a member from the
document. *[Figure 8, column 7, lines 5-7] (“removing a member”)*
8. **As per dependent claim 6 the combination of Carter, Rider and Frey**
discloses a method as applied to claims above. Furthermore, Carter
discloses the method further comprising: storing the member definition
remotely from the document. *[column 14, lines 35-38]*
9. **As per dependent claim 7 the combination of Carter, Rider and Frey**
discloses a method as applied to claims above. Furthermore, Carter
discloses the method further comprising: storing the member definition in
the document. *[Column 14, lines 31-34] (“In one embodiment, linking is
accomplished by storing the encrypted data portion 94 and the prefix portion 92
(including one or more member definitions 96) together in a file on a disk, tape, or
other conventional storage medium.”)*
10. **As per dependent claim 8 the combination of Carter and Frey** discloses a
method as applied to claims above. Furthermore, Carter discloses the
method further comprising: further comprising:

encrypting the document; and linking the member definition with a public key and a private key.*[column 11, lines 61- column 12, lines 7]*

11. **As per claims 9-10 the combination of Carter, Rider and Frey** discloses a method as applied to claims above. Furthermore, Rider discloses the method, further comprising: determining a second access right for the user; building a second member definition using the second access right; and linking the second member definition to a second portion of a document [Paragraph 0034-0035 paragraph 0044, figure 4A].
12. **Claims 11-21** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Stephen R. Carter** (hereinafter referred as **Carter**)(U.S. Patent No. 5,787,175) (Date of patent 28, 1998), in view of **Rider** (hereinafter referred to as **Rider**) (U.S. Patent Publication 2006/0173999 A1) (filed on 08/07/2003, claims priority of a provisional application filed on 08/07/2002)
13. **As per independent claim 11 Carter** discloses a method for controlling access to a document, [Abstract] comprising:
 - **A document comprising a first data and a second data.***[“the documents, which are indicated as 4, ref. Num “92” could be more than one as it is indicated on column 14, lines 23-24 and figure 4-6, the system builds one or more member definitions which is associated with one or more documents.]*

Art Unit: 2432

a first member definition [figure 5, ref. Num "96", "Member definition "]
associated with the first data[See figure 4, ref. Num "92"/"document "]
wherein the first member definition contains a first user identifier [Figure 5, ref. Num "98"] **and a first access right for a first user for the first data** [Figure 5, ref. Num "100"; see the "encrypted document key" which is encrypted by the member's public key. Only the Member who has access to the information could use his corresponding private key to decrypt and get the document key which allows the member to access the document. In particular see the following which is disclosed on column 13, lines 64-column 14, lines 5, "The encrypted document key 100 is formed by encrypting the document key obtained during the step 110 with the public key of the member in question, which was obtained during the step 116. Note that the underlying document key is the same for each member of the collaborative group, but the encrypted form 100 of the document key is unique to each member. Those of skill in the art will appreciate. that the encrypted document key 100 can be decrypted only by using the private key 80 that corresponds to the public key 78 used to encrypt the document-key."];

As it is indicated 14, lines 23-24 and figure 4-6, the system builds one or more member definitions. And the member definitions shown on figure 5, is associated to the documents shown on figure 4. Even though only one document is shown on figure 4, ref. Num "54, 90" the system is built for one or more documents. See the documents described on column 9, lines 35.

Thus the following is also correct.

a second member definition [figure 5, ref. Num “96”, “Member definition “]
associated with the second data [See figure 4, ref. Num “92”/”document “],
wherein the second member definition contains a second user
identifier[Figure 5, ref. Num “98”] **and a second access right for a second**
user for the second data; [Figure 5, ref. Num “100”; see the “encrypted
document key” which is encrypted by the member’s public key. Only the Member
who has access to the information could use his corresponding private key to
decrypt and get the document key which allows the member to access the
document. In particular see the following which is disclosed on column 13, lines
64-column 14, lines 5, “The encrypted document key 100 is formed by encrypting
the document key obtained during the step 110 with the public key of the member
in question, which was obtained during the step 116. Note that the underlying
document key is the same for each member of the collaborative group, but the
encrypted form 100 of the document key is unique to each member. Those of skill
in the art will appreciate. that the encrypted document key 100 can be decrypted
only by using the private key 80 that corresponds to the public key 78 used to
encrypt the document-key.”];

Carter does not explicitly disclose

Wherein the document has the first data portion and a second data portion,
receiving a request from the user to access the document; comparing the
request with the access right; and allowing access to only the first data portion
in accordance with the access right

However, in the same field of endeavor, **Rider** discloses,

Linking the member definition to a first data portion of a document, wherein the document has the first data portion and a second data portion, [paragraph 0044, figure 4A & 0034-0035] *(As shown, document 400 includes descriptor portion 402 and data portion 404. Descriptor portion 402 can include basic information about the device and its operation whereas data portion 404 can include actual data, which can be employed by specific applications. Portion 406 is a portion of data 404 that has its access governed in accordance with the principles of tier two security as described herein. That is, **one or more access rights can be associated with portion 406**. Although one portion 406 is shown, an ordinarily skilled artisan will appreciate that the same or other access rights can govern other portions of data portion 404.)*

Receiving a request from the user to access the document; comparing the request with the access right; and allowing access to only the first data portion in accordance with the access right [Paragraph 0034-0035 paragraph 0044, figure 4A] *(On paragraph 0034, the following has been disclose. Moreover, security manager 170 can permit, restrict or completely deny a user **request to access one or more documents** as well as the contents of those documents. A document or a portion thereof can represent a command for, or a configuration of, one of devices 135 such as a router or switch. Security manager 170 governs by determining whether a particular user has access rights to a specific network resource, **a particular document or only a portion of a document. Furthermore on paragraph 0035, the following has been disclosed.** “By restricting access in relation to a document's content, a more fine-grained approach to configuring, managing and monitoring network resources is*

*realized. Hence, tier two security restricts a user to data **constituting a portion of an entire document rather than providing complete or no access to that document.** For example, FIG. 4A depicts **document portion 406 that is accessible. Note that other portions of document 400 are not necessarily accessible to that user.**")*

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the feature such as linking the member definition to a first data portion of a document, wherein the document has the first data portion and a second data portion and receiving a request from the user to access the document; comparing the request with the access right; and allowing access to only the first data portion in accordance with the access right as per teachings of **Rider** into the method as taught by **Carter**, in order to provide a more fine-grained access control to the resources (portions of documents) [See For instance *Rider* on paragraph 0035].

14. As per independent claim 21 Carter discloses a method for controlling access to a document, [Abstract] comprising:

- **Determining an access right for a user; (Column 12, lines 56-63; column 15, lines 62-67; abstract and column 8, lines 27-29) (Access Control Methods FIGS. 4-9 illustrate one method according to the present invention for controlling collaborative access to the work group document 90. In particular, the method includes computer-implemented steps for collaboratively encrypting the**

document 90 (FIG. 6) and steps for restricting access to the data portion 94 of the collaboratively encrypted document (FIG. 9)).

- **building a member definition** [Figure 5, see “member definition”
comprising a member identifier [Figure 5, ref. Num “98”, See “member identifier”], **an access control** [See column 12, lines 56-57; column 13, lines 52-62, see figure 5, ref. Num 100, “encrypted document key” signed by the public key of the member. Only the member with the corresponding private key can access the document. In particular see the following which is disclosed on column 13, lines 64-column 14, lines 5, “The encrypted document key 100 is formed by encrypting the document key obtained during the step 110 with the public key of the member in question, which was obtained during the step 116. Note that the underlying document key is the same for each member of the collaborative group, but the encrypted form 100 of the document key is unique to each member. Those of skill in the art will appreciate. that the encrypted document key 100 can be decrypted only by using the private key 80 that corresponds to the public key 78 used to encrypt the document-key. ”See also “collaborative access controller 44” which is described on column 6, lines 11-22 as the access controller which restrict access to the members only. Non members are restricted from accessing the information. See for instance the following disclosed on column 6, lines 11-12, “users who are currently members of a collaborative group can readily access the information, while users who are not currently members of the group cannot”]
and a digital signature, [See also figure 5, ref. Num “102”, “encrypted message digest”, signed by the private key. In particular see what is disclosed on column

Art Unit: 2432

14, lines 15-21, *“the encrypted message digest 102 is formed by generating a message digest based on the current contents of the data portion 94 of the document 90 and then encrypting that message digest with the private key 80 of the member who is signing the document 90.”* See also the abstract and column 6, lines 11-12, *“collaborative signatures, such that members of the group can digitally sign a particular version of the data portion. These collaborative signatures can then be used to advantage in ways similar to conventional individual digital signatures. For instance, the collaborative signatures can be used to identify the signing member.”*] **and associating the member definition with the user.** [Figure 5 and column 6, lines 11-22, See *“Users who are currently members of a collaborative group can readily access the information, while users who are not currently members of the group cannot”*]

and

- **Linking the member definition to a portion of a document.** [Figure 6, ref. Num “120”] (*“Link member definition(s) with document.”*)

Carter does not explicitly disclose

linking the member definition to a first data portion of a document, wherein the document has the first data portion and a second data portion, receiving a request from the user to access the document; comparing the request with the access right; and allowing access to only the first data portion in accordance with the access right

However, in the same field of endeavor, **Rider** discloses,

Linking the member definition to a first data portion of a document, wherein the document has the first data portion and a second data portion, [paragraph 0044, figure 4A & 0034-0035] *(As shown, document 400 includes descriptor portion 402 and data portion 404. Descriptor portion 402 can include basic information about the device and its operation whereas data portion 404 can include actual data, which can be employed by specific applications. Portion 406 is a portion of data 404 that has its access governed in accordance with the principles of tier two security as described herein. That is, **one or more access rights can be associated with portion 406**. Although one portion 406 is shown, an ordinarily skilled artisan will appreciate that the same or other access rights can govern other portions of data portion 404.)*

Receiving a request from the user to access the document; comparing the request with the access right; and allowing access to only the first data portion in accordance with the access right [Paragraph 0034-0035 paragraph 0044, figure 4A] *(On paragraph 0034, the following has been disclose. Moreover, security manager 170 can permit, restrict or completely deny a user **request to access one or more documents** as well as the contents of those documents. A document or a portion thereof can represent a command for, or a configuration of, one of devices 135 such as a router or switch. Security manager 170 governs by determining whether a particular user has access rights to a specific network resource, **a particular document or only a portion of a document. Furthermore on paragraph 0035, the following has been disclosed.** “By restricting access in relation to a document's content, a more fine-grained approach to configuring, managing and monitoring network resources is*

*realized. Hence, tier two security restricts a user to data **constituting a portion of an entire document rather than providing complete or no access to that document.** For example, FIG. 4A depicts **document portion 406 that is accessible. Note that other portions of document 400 are not necessarily accessible to that user.**")*

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the feature such as linking the member definition to a first data portion of a document, wherein the document has the first data portion and a second data portion and receiving a request from the user to access the document; comparing the request with the access right; and allowing access to only the first data portion in accordance with the access right as per teachings of **Rider** into the method as taught by **Carter**, in order to provide a more fine-grained access control to the resources (portions of documents) [See For instance *Rider* on paragraph 0035]

15. **As per dependent claims 12-13 the combination of Carter and Rider** discloses a method as applied to claims above. Furthermore, **Rider** discloses the method, wherein the access controller limits access to the document in accordance with the first access right and the second access right. And, wherein the first user identifier and the second user identifier identify the same user and the first access right and the second access right identify different access rights [Paragraph 0034-0035 paragraph 0044, figure 4A].
16. **As per dependent claim 14 the combination of Carter and Rider** discloses a method as applied to claims above. Furthermore, **Carter** discloses the

Art Unit: 2432

method wherein the first member definition contains a digital signature.

[Abstract and figure 10, ref. Num "184"]

17. **As per dependent claim 15 the combination of Carter and Rider discloses a method as applied to claims above. Furthermore, Carter discloses the method wherein the first member definition and second member definition are stored remotely from the document.** *[column 14, lines 35-38]*
18. **As per claim dependent 16 the combination of Carter and Rider discloses a method as applied to claims above. Furthermore, Carter discloses the method where in the first and second the member definition are stored in the document.** *[Column 14, lines 31-34] ("In one embodiment, linking is accomplished by storing the encrypted data portion 94 and the prefix portion 92 (including one or more member definitions 96) together in a file on a disk, tape, or other conventional storage medium.")*
19. **As per dependent claims 17-20 the combination of Carter and Rider discloses a method as applied to claims above. Furthermore, Carter discloses the method wherein the document is tagged document/XML document/text document/binary document.** *[Column 9, lines 32-61]*

Conclusion

Art Unit: 2432

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-2723806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm). The fax phone number for Examiner Lemma is 703-872-9306.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-273-8300.

/Samson B Lemma/
Examiner, Art Unit 2432

/Gilberto Barron Jr./
Supervisory Patent Examiner, Art Unit 2432